(19) KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 000038712 A
(43)Date of publication of application: 05.07.2000

(21)Application number: 980053793
(22)Date of filing: 08.12.1998

(71)Applicant: SAMSUNG ELECTRONICS CO., LTD.
(72)Inventor: KONG, IN UK
KIM, SEUNG JIN

(51)Int. Cl G06F 17/00

(54) METHOD AND MICRO CONTROLLER HAVING REPRODUCTION PREVENTING FUNCTION

(57) Abstract:

PURPOSE: A micro controller having a reproduction preventing function, and a method therefor are provided so that reproduction of a program code and an encoder can be prevented, and a read-only-memory(ROM) storing the program code can be externally installed.

CONSTITUTION: A program processing unit(10) processes an application program by using a predetermined key data and an encoded data. An encoder(20) encodes the key data from the program processing unit(10), and outputs an encoded data. As a result, it is possible to prevent the program code and the encoder(20) from being reproduced.

Legal Status

Date of request for an examination ( )
Notification date of refusal decision ( )
Final disposal of an application (application)
Date of final disposal of an application ( )
Patent registration number ( )
Date of registration ( )
Number of opposition against the grant of a patent ( )
Date of opposition against the grant of a patent ( )
Number of trial against decision to refuse ( )
Date of requesting trial against decision to refuse ( )
Date of extinction of right ( )

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 17/00

(11) 공개번호 특2000-0038712
(43) 공개일자 2000년07월05일

(21) 출원번호 10-1998-0053793
(22) 출원일자 1998년12월08일

(71) 출원인 삼성전자 주식회사 윤종용
경기도 수원시 팔달구 매탄3동 416
(72) 발명자 공인욱
경기도 용인시 기흥읍 농서리 산 24
김승진
경기도 용인시 기흥읍 농서리 산 24
(74) 대리인 권석흠, 이영필, 정상빈

심사청구 : 없음

(54) 복제 방지 기능을 갖는 마이크로 콘트롤러 장치 및 그의 복제방지 방버뷰

요약

복제 방지 기능을 갖는 마이크로 콘트롤러 장치 및 그의 복제 방지 방법이 개시된다. 이 장치는, 소정의 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 프로그램 처리부 및 프로그램 처리부로부터 출력되는 키 데이타를 암호화하여 암호화된 데이타로서 출력하는 암호화부를 구비하는 것을 특징으로 한다. 그러므로, 프로그램 코드 및 암호화부의 복제를 방지할 수 있도록 하고, 프로그램 코드를 저장하는 롬을 외부에 마련할 수 있도록 하는 효과가 있다.

대표도

도1

명세서

도면의 간단한 설명

도 1은 본 발명에 의한 복제 방지 기능을 갖는 마이크로 콘트롤러 장치의 개략적인 블럭도이다.

도 2는 도 1에 도시된 장치의 복제를 방지하는 본 발명에 의한 복제 방지 방법을 설명하기 위한 플로우차트이다.

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 마이크로 콘트롤러 장치(MCU:Micro Controller Unit)에 관한 것으로서, 특히, 복제 방지 기능을 갖는 마이크로 콘트롤러 장치 및 그의 복제 방지 방법에 관한 것이다.

장기간에 걸쳐 많은 노력과 비용을 들여 개발된 마이크로 콘트롤러 장치가 내장된 어플리케이션 제품이 시장이 판매될 경우, 불과 수 개월만에 동일한 기능을 갖는 복제된 제품이 더욱 저렴한 가격에 시중에서 불법으로 유통될 수 있다. 이는, 마이크로 콘트롤러에 프로그램 코드의 복제가 용이할 뿐만 아니라, 마이크로 콘트롤러 응용 제품을 다른 제품들과 함께 조립하면 복제가 가능해지기 때문이다.

종래에, 마이크로 콘트롤러 장치의 복제를 방지하는 방법으로서, 프로그램 논리 디바이스(PLD:Programmable Logic Device)등을 사용하여 그 장치를 숨기는 방법과 마이크로 콘트롤러에 내장된 롬(ROM)을 사용하여 프로그램 코드를 숨기는 방법들이 있다. 그러나, 전자의 방법은 타인이 입/출력 신호를 분석하여 PLD를 복제 가능한 문제점이 있고, 후자의 방법은 마이크로 콘트롤러 장치 내부의 롬은 크기가 적으므로 큰 용량의 프로그램 코드를 저장할 수 없을 뿐만 아니라 마이크로 콘트롤러 디버깅(dubugging) 장치에 의해 프로그램 코드의 복제가 가능해지는 문제점이 있다.

발명이 이루고자하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는, 그 하드웨어나 프로그램 코드의 복제를 방지하는 기능을 갖는 마이크로 콘트롤러 장치를 제공하는 데 있다.

본 발명이 이루고자 하는 다른 기술적 과제는, 상기 마이크로 콘트롤러 장치의 복제를 방지하는 마이크로 콘트롤러 장치의 복제 방지 방법을 제공하는 데 있다.

발명의 구성 및 작용

상기 과제를 이루기 위한 본 발명에 의한 복제 방지 기능을 갖는 마이크로 콘트롤러 장치는, 소정의 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 프로그램 처리부 및 상기 프로그램 처리부로부터 출력되는 상기 키 데이타를 암호화하여 상기 암호화된 데이타로서 출력하는 암호화부로 구성되는 것이 바람직하다.

상기 다른 과제를 이루기 위해, 외부로부터 주어지는 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 프로그램 처리부 및 상기 키 데이타를 암호화하여 상기 암호화된 데이타를 생성하는 암호화부를 갖는 마이크로 콘트롤러 장치의 복제를 방지하는 본 발명에 의한 복제 방지 방법은, 상기 프로그램 처리부에서 상기 응용 프로그램을 처리할 때, 상기 암호화된 데이타 및 상기 키 데이타가 존재하는가를 판단하는 단계와, 상기 암호화된 데이타 및 상기 키 데이타가 존재할 경우, 존재하는 암호화된 데이타가 원하는 데이타인가를 판단하는 단계 및 상기 존재하는 암호화된 데이타가 상기 원하는 데이타가 아니거나, 상기 암호화된 데이타 또는 상기 키 데이타가 존재하지 않은 경우, 상기 응용 프로그램의 처리를 중지시키는 단계로 이루어지는 것이 바람직하다.

이하, 본 발명에 의한 복제 방지 기능을 갖는 마이크로 콘트롤러 장치의 구성 및 동작을 첨부한 도면을 참조하여 다음과 같이 설명한다.

도 1은 본 발명에 의한 복제 방지 기능을 갖는 마이크로 콘트롤러 장치의 개략적인 블럭도로서, 프로그램 처리부(10), 암호화부(20), 주변부(30) 및 어드레스/데이타/콘트롤 버스(50)로 구성된다. 이 때, 도 1에 도시된 장치는 집적(40)화될 수 있다.

도 1에 도시된 프로그램 처리부(10)는 소정의 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 역할을 한다. 여기서, 소정의 키 데이타는 도 1에 도시된 장치의 제작자에 의해 외부로부터 입력된다. 이 때, 암호화부(20)는프로그램 처리부(10)로부터 입력한 키 데이타를 암호화하고, 암호화된 결과를 암호화된 데이타로서 프로그램 처리부(10)로 출력한다. 예를 들어, 암호화부(20)는 예를 들면 "0x123456789ABCDE12"와 같은 키 데이타를 프로그램 처리부(10)로부터 입력하여 예를 들면 "0x875745863950A486" 같은 데이타로 암호화한다. 결국, 제작자만이 알고 있는 키 데이타를 암호화하여 숨김으로써, 프로그램 코드 및/또는 암호화부(20)의 복제를 방지할 수 있다.

이 때, 여러가지 방법에 의해, 암호화된 데이타 "0x875745863950A486"가 노출되었다 하더라도, 암호화된 데이타를 생성하는 키 데이타를 알 수 없으면 프로그램을 수행할 수 없도록 한다. 이를 위해, 후술되는 바와 같이, 프로그램의 곳곳에서 암호화된 데이타 즉, "0x875745863950A486"이 읽혀지는가를 검사하고, 검사된 결과에 따라 정품 여부를 판단하고, 그 판단 결과에 따라 프로그램이 수행될 수 있도록 한다.

이 때, 프로그램 처리부(10)는 외부로부터 주어지는 소정의 키 데이타를 암호화부(20)에 단지 한번만 기입할 수 있도록 구현한다. 왜냐하면, 키 데이타와 암호화된 데이타의 상관관계를 분석하여 암호화부(20)를 유추할 수 있기 때문에, 그 상관관계를 분석하기 어렵도록 하기 위해서이다. 그러므로, 허용되지 않은 사용자 즉, 불법 복제자가 키 데이타와 암호화된 데이타의 상관관계를 분석하기 위한 자료를 수집하고자 할 경우, 그 복제자는 매번 칩(40)을 교환해야 하므로, 많은 시간과 금전을 소비할 것이다.

이하, 도 1에 도시된 장치의 본 발명에 의한 복제 방지 방법을 첨부한 도면을 참조하여 다음과 같이 설명한다.

도 2는 도 1에 도시된 장치의 복제를 방지하는 본 발명에 의한 복제 방지 방법을 설명하기 위한 플로우차트로서, 키 데이타 및 암호화된 데이타를 이용하여 마이크로 콘트롤러 장치의 복제를 방지하는 단계(제50 ~ 제54 단계)로 이루어진다.

도 1 및 도 2를 참조하면, 프로그램 처리부(10)에서 응용 프로그램을 처리할 때, 암호화부(20)에서 암호화된 데이타 및 외부에서 주어진 키 데이타가 존재하는가를 판단한다(제50 단계). 이는 응용 프로그램의 중간 중간에 암호화된 데이타를 체크하고, 장치의 초기 상태에서 키 데이타를 체크하도록 함으로써 실현될 수 있다. 여기서, 응용 프로그램은 프로그램 처리부(10)의 내부 또는 외부에 마련될 수 있는 롬에 저장된다.

만일, 암호화된 데이타 및 키 데이타가 존재할 경우, 존재하는 암호화된 데이타가 원하는 데이타인가를 판단한다(제52 단계). 즉, 암호화된 데이타가 정상적인 키 데이타를 암호화하였을 때 얻어지는 데이타인가를 판단한다.

만일, 암호화된 데이타가 정상적인 데이타인 경우, 프로그램 처리부(10)는 해당하는 응용 프로그램을 정상적으로 수행한다. 그러나, 존재하는 암호화된 데이타가 원하는 데이타가 아니거나, 암호화된 데이타 또는 키 데이타가 존재하지 않은 경우, 프로그램 처리부(10)는 응용 프로그램의 처리를 중지한다(제54 단계).

발명의 효과

이상에서 설명한 바와 같이, 본 발명에 의한 마이크로 콘트롤러 장치 및 그의 복제 방지 방법은 집적회로로 구현될 수 있는 마이크로 콘트롤러 장치의 내부에 암호화부를 존재시키기 때문에 암호화부의 입/출력 신호와 상관관계를 근본적으로 관찰하지 못하게 하여 암호화부의 복제를 방지하고, 마이크로 콘트롤러 장치를 디버깅 장비를 이용하여 해독한다 할지라도 암호화된 데이타만을 읽을 수 있을 뿐 키 데이타를 알지 못하면 복제된 프로그램을 사용할 수 없도록 하고, 프로그램 코드의 복제를 무용화시킬 수 있기 때문에 프로그램 코드를 외부의 롬에 제한없이 저장시킬 수 있는 효과가 있다.

(57) 청구의 범위

청구항 1. 소정의 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 프로그램 처리부; 및

상기 프로그램 처리부로부터 출력되는 상기 키 데이타를 암호화하여 상기 암호화된 데이타로서 출력하는 암호화부를 구비하는 것을 특징으로 하는 복제 방지 기능을 갖는 마이크로 콘트롤러 장치.

청구항 2. 제1 항에 있어서, 상기 프로그램 처리부는 외부로부터 주어지는 상기 소정의 키 데이타를 상기 암호화부에 한번만 출력하는 것을 특징으로 하는 마이크로 콘트롤러 장치.

청구항 3. 외부로부터 주어지는 키 데이타 및 암호화된 데이타를 이용하여 응용 프로그램을 처리하는 프로그램 처리부 및 상기 키 데이타를 암호화하여 상기 암호화된 데이타를 생성하는 암호화부를 갖는 마이크로 콘트롤러 장치의 복제를 방지하는 복제 방지 방법에 있어서,

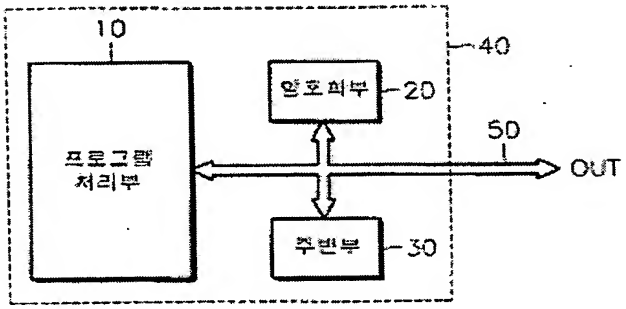
상기 프로그램 처리부에서 상기 응용 프로그램을 처리할 때, 상기 암호화된 데이타 및 상기 키 데이타가 존재하는가를 판단하는 단계;

상기 암호화된 데이타 및 상기 키 데이타가 존재할 경우, 존재하는 암호화된 데이타가 원하는 데이타인가를 판단하는 단계; 및

상기 존재하는 암호화된 데이타가 상기 원하는 데이타가 아니거나, 상기 암호화된 데이타 또는 상기 키 데이타가 존재하지 않은 경우, 상기 응용 프로그램의 처리를 중지시키는 단계를 구비하는 것을 특징으로 하는 마이크로 콘트롤러 장치의 복제 방지 방법.

도면

도면1



도면2